ANALYSIS AND EVALUATION SNORT, BRO, AND SURICATA AS INTRUSION DETECTION SYSTEM BASED ON LINUX SERVER

Paper

Department of Informatics
Faculty of Communications and Informatics

By:

M. Faqih Ridho
Fatah Yasin, S.T., M.T.
Yusuf Sulistyo N, S.T., M.Eng

DEPARTMENT OF INFORMATICS
FACULTY OF COMMUNICATIONS AND INFORMATICS
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2014

VALIDATION

"ANALYSIS AND EVALUATION SNORT, BRO, AND SURICATA AS INTRUSION DETECTION SYSTEM BASED ON LINUX SERVER"

Presented by:

M. FAQIH RIDHO

L200090136

First Advisor	Second Advisor
Fatah Yasin, S.T, M.T	**Yusuf Sulistyo Nugroho, S.T, M.Eng**
NIK : 738	**NIK : 100.1197**

has been approved and legalized on:

Day :

Date :

This final project report has been accepted as the requirement for the bachelor degree

Head of Department of Informatics

Dr. Heru Supriyono, M.Sc.

NIK : 970

ANALYSIS AND EVALUATION SNORT, BRO, AND SURICATA AS INTRUSION DETECTION SYSTEM BASED ON LINUX SERVER

M. Faqih Ridho, Fatah Yasin, S.T., M.T., Yusuf Sulistyo N, S.T., M.Eng

Department of Informatics, Faculty of Communications and Informatics

Universitas Muhammadiyah Surakarta

Email : ahmad_idho@yahoo.co.id

ABSTRACT

Security and confidentiality of data on computer networks is currently a problem that continues to grow. Installation of firewalls, antivirus, IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) and various other security applications often require the best available installation cost is not small. Open source is the best solution to address the security issues that expensive. Intrusion Detection System is a system designed to collect information about the activities in the network, analyzing information, and give a warning. Snort, Bro and Suricata is an open source Intrusion Detection System. By comparing how the installation, configuration, warnings are displayed, and the resulting information can to know the advantages and disadvantages of snort Snort, Bro and Suricata as Intrusion Detection System.

There are two stages of testing, such as scanning and penetration. Phase scanning is a scan of all ports, scanning is done by using NMAP application which is found on Armitage. Stage penetration is done by using the menu hail mary which is contained in Attack tab, hail mary is used to try all the exploits against computer target.

Based on Scanning and penetration process, Snort detects 926 alert, Suricata detects 1218 alerts and Bro detects 128 alerts. Snort and Suricata ease to install and update rule, Bro requires the least amount of resources.

Key words: Bro, Intrusion Detection System, Snort, Suricata

BACKGROUND OF STUDY

The security and confidentiality problem of computer network is improving now. In the last years, the dangerous traffic like malicious and ddos (distributed denial of service) is improving. There are companies which offer some services to public, getting attack which is caused they cannot offer user demand (KasperskyLab, 2013).

The installation of firewall, antivirus, IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) and other security applications are available. But they are expensive. For rich companies, there will be not problem to install an expensive security application. But it will be a big problem for poor companies. Open source application can be a solution. Almost open source applications are free, and user can develop the application.

Nowadays, IDS is one of famous security tools which are used. IDS prevent hacker or intruder to attack the company's system. Administrator can collect information about attack from IDS. Administrator also uses it for knowing whether people try to attack the network or specific host.

There are some IDS open source application such as Snort, Bro, Ossec, Prelude, and Suricata. The characteristic of good IDS applications are they have accuracy, performance, completeness, fault tolerance, and scalability. With these characteristics, IDS application can help administrator to minimize some errors in taking action.

Based on the facts above, the writer tries to make analysis and evaluation from three applications. Applications are Snort, Bro, Suricata.

RESEARCH STUDY

Syujak (2012) said that the security of the computer network is a very important part to maintain the validity and integrity of the data. Besides, it also guarantees the services availability for its users. An attack on the computer network server can occur at any time, either when administrators are working or not working. Thus the server security system is needed to detect whether each incoming packet is the actual data packets. If the packet is a attacker's packet data, then system will block attacker's IP. The security system is Snort. There are some disadvantages of snort, such as snort can only detect flooding data based on size which is sent. It causes that if there is a packet is sent simultaneously with smaller size of rule (rule is applied to snort) then create flooding. It cannot be detected by system. The result is the system will not give any action. It is caused that the system doesn't get an alert about flooding data attack.

Firdaus (2011), said that in the company, network security system, Internet Service Provider (ISP) is an important factor to guarantee the stability, integrity, and data validity. The implementation of Intrusion Detection System based on Snort can save money to buy software. It is caused that snort is free software and can be relied to detect security attack. Snort's main setting is in the network setting and the rule of existing snort. Snort IDS can detect and cannot detect the attack. It

depends on the availability of appropriate rule. Testing in the IDS system is done by some attack patterns. It is done to test the ability of snort to detect an attack against the security system. Based on the testing result among IDS Snort system with port scan, virus test, buffer overflow, SQL injection, and accessing database, snort can give an alert if there is an attack to the network system.

Day and Burns (2011) said that in performance of testing of Snort 2.8.5.2 and Suricata 1.0.2 in Ubuntu 10.04 which is run in Intel Xeon Quad-Core 2.8 GHz with RAM 3 GB. Using Metasploit as alert injection. Testing Variable is as performance and accuracy. It is gotten that the use of sources of snort is the most efficient. In operation, multi-CPU scope, Suricata is the most accurate. It is caused that suricata do a little bit false negative alert. In the other hand, they conclude that in the four-core scope, suricata is slower than snort in single-core scope. It happens when suricata proceed 2 Gigabytes data.

METHOD

The steps of the research described in the flowchart figure 1.

Figure 1: The Flowchart of the Research

RESULT AND ANALYSIS

There are two phases of testing. The first stage is intense scan all TCP ports. The second stage is the hail mary attack. Research results which are obtained after testing the system are as follows:

A. Result

1. Scanning

The purpose of scanning is to see which port are open. The results of the scanning process are in two computers. The computer with the IP Addres 192.168.5.1 is a computer server where the IDS application is installed. The computer with the IP address

192.168.5.15 is the client computer that is used for scanning and penetration. Open port is port 22, 80, 443, 444, 514, 3154, 7734, and 7736 ports. Open ports is used as a way to do exploits.

2. Penetration Step

Penetration is done by sending all the exploits from the client computer to the server computer through open ports. Open ports are obtained from the scanning stage. The delivery of exploits has the objective to do penetration. Penetration was conducted in order to find the vulnerability of a computer server. Exploits is delivered automatically adjusted by Armitage. Adjustments are made according to a computer server operating system.

3. The Use of Resource

The use of resource that is observed of this research is the use of CPU and RAM. It is based on before testing and testing process of the system.

Table 1: Use of Resource

IDS / Parameter	Snort	Bro	Suricata
CPU usage in a normal state	46 %	46,4 %	44,4 %
CPU usage when testing	68 %	58,2 %	99 %
RAM usage in a normal state	71,6 %	46,4 %	69,9 %
RAM usage when testing	76,1 %	55 %	73 %

4. Warning Detection

Detected warning is grouped into three groups. The groups are high alert, medium alert, and low alert. Below is alert which is detected by IDS application.

Table 2: Warning Detection

IDS / Alert	Snort	Bro	Suricata
High	1 %	0 %	2 %
Medium	3 %	0 %	4 %
Low	96 %	100 %	94 %

B. Discussion

The research was conducted through several stages. Stages include the design, configuration and testing. There is some error occurs when installing a IDS supporting package and the IDS application. On the other hand there is a manual on every IDS application. It eases the process of installation of the IDS application on the computer server.

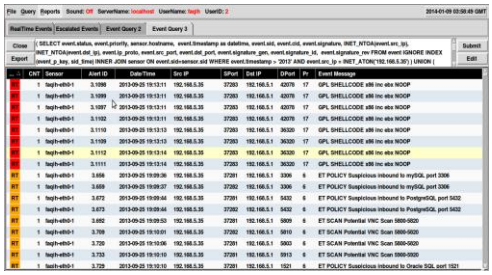
There are some problems in installing the package as a supporter of IDS through "apt-get install". However error can be resolved by following the guidance contained in the Ubuntu website.

There are problems when testing Snort, Suricata and Bro. These problems include the use of a computer server. This causes the researchers had difficulty to read logs of Snort and Suricata. It is caused of Snort and Suricata uses the same frontend application to read the log. As a result, testing was conducted using a different IP address for each IDS application.

Another issue is the use of big resource when testing Suricata. This causes computer hung during testing

time. It has an impact on the computer server. The computer can not perform services as in normal state.

IDS application can only give a warning to the traffic that occurs on the network. All traffic that occurs on the network will be recorded into a log by IDS. It can be used to perform analysis in case of an attack on a computer. It can help to analyze the attack.



update rule. In the other hand, it needs large resource. While Bro though in terms of the installation requires more time, but the resource usage Bro require less than Snort and Suricata

CONCLUSION

Based on the result, the writer concludes that:

1. Snort, Bro and Suricata can be implemented in Ubuntu Server 12.04 Operating system as Intrusion Detection System application. This application to detect penetration from client computer.
2. Based on Scanning and penetration process, Snort 2.9.5.3 detects 926 alert with 8 high alerts, 29 medium alerts, and 889 low alert. Suricata 1.4.5 detects 1218 alerts with 22 high alerts, 44 medium alerts and 1152 low alerts. Bro detects 128 low alerts.
3. Snort, Bro dan Suricata has each advantages and disadvantages. Snort and Suricata ease to install and

BIBLIOGRAPHY

Ariyus, Dony. 2007. "Intrusion DetectionSystem Sistem Pendeteksi Penyusup Pada Jaringan Komputer". Yogyakarta : Andi.

Athailah. 2012. "*Buku Pintar Ubuntu".* Jakarta Selatan: Media Kita.

Carr, Jeffrey. 2007. "Snort: Open Source Network Intrusion Prevention".

Day, D., & Burns, B. 2011. "*A performance analysis of snort and suricata network intrusion detection and prevention engines*". IDCS 2011, the Fifth International Conference on Digital Society, Gosier, Guadeloupe, France. 187–192.

Debar, Herve & Dacier, Marc & Wespi, Andreas. 1999. "*Towards a taxonomy of intrusion-detection systems".*

Firdaus, Atiq Zahrial. 2011. "*IMPLEMENTASI SNORT SEBAGAI TOOL INTRUSION DETECTION SYSTEM PADA SERVER FREEBSD DI PT. POWER TELECOM".* Skripsi. Skripsi. Surakarta: Universitas Muhammadiyah Surakarta.

Gagné, Marcel. 2006. "Moving to Ubuntu Linux**"**

Karen. 2007. " Guide to Intrusion Detection and Prevention Systems (IDPS)" *Computer Security Resource Center*

Kristanto, Andri. 2003. "*Kemanan Data Pada Jaringan Komputer".* Yogyakarta: Gava Media.

Paxson, Vern. 1999. "Bro: A System for Detecting Network Intruders in Real-time". Computer Networks : Vol 31.

Rafiudin, Rahmat. 2010. *"MENGGANYANG HACKER dengan SNORT".* Yogyakarta: Andi.

SUPARSIN, HERU dkk. 2011. *PEMILLIHAN IDS (INTRUSION DETECTION SYSTEM) SEBAGAI SISTEM KEAMANAN JARINGAN SERVER DI POLITEKNIK BATAM*. Batam: Politeknik Batam.

Syujak, Ahmad Rois. 2012. "*DETEKSI DAN PENCEGAHAN FLOODING DATA PADA JARINGAN KOMPUTER*. Skripsi. Surakarta: Universitas Muhammadiyah Surakarta.

OECD Ministerial Background Report. (2008). DSTI/ICCP/REG(2007)5/FINAL. "malicious software (malware): A security threat to the Internet economy".

OISF. "About Suricata". www.openinfosecfoundation.org. Diakses pada tanggal 20 Mei 2014.

Wagito. 2007. "*Jaringan Komputer Teori dan Implementasi Berbasis Linux".* Yogyakarta: Gava Media.

BIODATA PENULIS

Nama	: M. Faqih Ridho
NIM	: L200090136
Tempat Lahir	: Brebes
Tanggal Lahir	: 29 Agustus 1989
Jenis Kelamin	: Laki-Laki
Agama	: Islam
Pendidikan	: S1
Jurusan / Fakultas	: Teknik Informatika / Komunikasi dan Informatika
Perguruan Tinggi	: Universitas Muhammadiyah Surakarta
Alamat Rumah	: Glempang, Pagojengan RT 06 RW 02 Paguyangan Brebes
No. HP	: 085743604912
Email	: ahmad_idho@yahoo.co.id